CONFERENCE REPORT

The Third International Virus Bulletin Conference

With the images of the *VB '92* conference still firmly implanted in one's mind, it is difficult to believe that all that Scottish merry-making happened over a year ago. Have 365 days really passed? Apparently so, as the conference went Dutch last month for *VB '93*.

The conference was held in The *Grand Hotel Krasnapolsky*, situated in the heart of Amsterdam. With over 150 delegates making the journey from twenty-four different countries, the conference took on not only a continental but a truly international flavour.

Man cannot live on viruses alone... or so the saying goes. With this in mind, the conference began with dinner for the speakers in the *Five Flies* restaurant, after a canal trip for both the delegates and the speakers, which gave everyone a chance to gain their bearings, and to sample the local brews. This trip was accompanied by a drizzly shower, which (with the Jenever flowing freely) dampened the coats but fortunately not the spirits of the delegates.

Conference Overview

According to many of the delegates at the conference, IT Managers now understand what they need to do in order to prevent virus attack, but want to know how to ensure that their carefully drawn-up policies are actually followed. 'We aren't interested in how Joe User's company places a copy of

Team *VB '93* (left to right): (Back row) Tim Winder, *Shell Nederland Informatiewerverking*, Stefano Toria, *CSI srl*, Jim Bates, *Bates Associates*. (Fourth Row) David Rischmiller, *Oxford University Computer Services*, John Walker, *ADS Computer Systems*, Jan Terpstra, *IBM Nederland NV*, George Guillory, *Paramax Space Systems*, Roger Marshallsay, *Secure Information Systems*, Rupert Goodwins, *PC Magazine*. (Third Row) Righard Zwienenberg, *Computer Security Engineers*, Steve White, *IBM*, Jan Hruska, *Sophos*, Philip Bancroft, *Digital Equipment Corporation*, Vesselin Bontchev, *Virus Test Centre*, Roger Riordan, *CYBEC Pty*. (Second Row) Fridrik Skulason, *Frisk Software*, Richard Ford, *Virus Bulletin*, Dmitry Gryaznov, *Russian Academy of Sciences*, Winn Schwartau, *InterPact Information Security*, Matthias Jänichen, *Virus Test Centre*, Ian Chambers, *ESA*, Rod Parkin, *Midland Bank*. (Front Row) Frans Veldman, *ESaSS BV*.

F-Prot on every workstation', commented one delegate. 'What we want is to understand how to enforce the rules, and what can go wrong.'

The conference attempted to answer some of these problems, but more than anything served to differentiate the needs of the users from those of the anti-virus industry. Exactly as last year, users are increasingly frustrated by the anti-virus manufacturers' schoolboy fascination with competing sizes of virus collections - what they need is a *solution*.

Up to Speed

The delegates had already been treated to the infamous Steve White-Jan Hruska Virus-101 course the evening before the conference began, but *IBM* wanted to reinforce this message. A good virus defence policy is built on several very simple precepts, and the opening talk by Jan Terpstra attempted to drum this maxim home.

However, a far more thorny problem is that of what to do when something has gone wrong. A virus is loose on your computer system. It is not identified by current anti-virus software, and is highly destructive. What should you do now? This is exactly the situation David Rischmiller, from *Oxford University Computer Services*, found himself in.

Summing up the situation in early 1991 at *OUCS*, Rischmiller was disarmingly frank. 'At the start of 1991 we were aware of viruses; we had been subscribers to the *Virus-l* mailing list for some time; we were giving anti-virus advice to our users; and were taking simple anti-virus precautions with the machines under our control which were available for public use. We had even made a start on producing a document about computer viruses and their prevention ... for all that, we were naïve about the issues.'

Rischmiller then went on to explain about the unforeseen problems which the virus (in this case, Spanish Telecom) caused within the university. One interesting side-effect of the problem was that the users became increasingly paranoid about the nature of the virus infection which was spreading throughout the university - a problem which PC support staff will know all too well.

One problem which seems set to affect *OUCS* for the foreseeable future is that of 'haunting' by the Spanish Telecom virus, as machines become infected from one of the many infected floppy diskettes which are mouldering in a forgotten corner of an office. 'If there has been a serious outbreak,' explains Rischmiller, 'everyone is eager to do the right thing, but as the memory fades, so does the enthusiasm. I don't think there is any way of stopping this in a university environment. You can take a horse to water...'

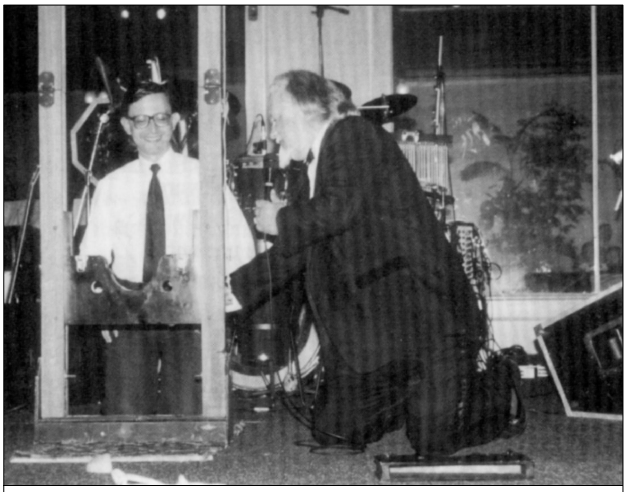
A Sense of Security

Not everyone in the anti-virus industry has the same perspective on how to go about preventing the spread of computer viruses. The most controversial talk of the conference was on an alternative approach to virus prevention.

Winn Schwartau, the cause of the furore, believes that the current approach to virus prevention is simply wrong, and that by using well known security techniques it is possible to limit the spread of computer viruses within an organisation. 'As most security professionals probably already know, I am not a big fan of virus busting', began Schwartau, before embarking on a no-holds-barred critique of the industry.

Schwartau argued that a better way to prevent viruses is to use a combination of the security systems one might find on a large mainframe system. He believes this is a better system for a number of reasons:

- It will cost less money than is currently spent on anti-virus software
- It will save the man-hours spent on keeping anti-virus software up to date
- It will provide protection against unknown viruses as well as known ones
- It will provide a number of additional benefits which are badly needed by the corporate IT manager.



As he was led to the Guillotine, Monsieur Bontchev was heard to mutter 'Let them use DEBUG...'

The delegates and speakers seemed to be divided by Schwartau's assertions. Vesselin Bontchev gave a lengthy multi-point argument against Schwartau (he did not agree with *any* of the points Schwartau raised!) and his views reflected those of several of the speakers and a proportion of the audience. However, the remainder of the delegates were very interested in what Schwartau's model had to offer. The acid test of his ideas will be how they fare on large systems over a period of time - meanwhile the jury is still out on this one. Debate over Schwartau's ideas continued through the rest of the conference.

Reviewing the Reviewers

On a more technical note, Vesselin Bontchev gave an informative account of how virus scanners should be tested. He explained that the biggest problem is maintaining a virus

collection: if the virus test-set used to examine anti-virus software is at fault, the test results are not valid.

However, the process of 'weeding' a large collection of the junk and joke programs which it contains is non-trivial. A typical 'virus collection' may consist of megabytes of data, much of which will not be of interest to the virus researcher - however, it all must be examined, in case it contains new viruses. Bontchev went on to describe how this should be done:

One of the most common mistakes to make when compiling a virus collection is the inclusion of first-generation virus droppers (which Bontchev further classifies as germs, droppers and injectors). The problem with such files is that although they replicate, they do not represent a typical infection, and therefore should not be included when testing scanners.

Bontchev concluded that even after many months of effort, the *Virus Test Centre* in Hamburg was still not ready to review products as thoroughly as he would like.

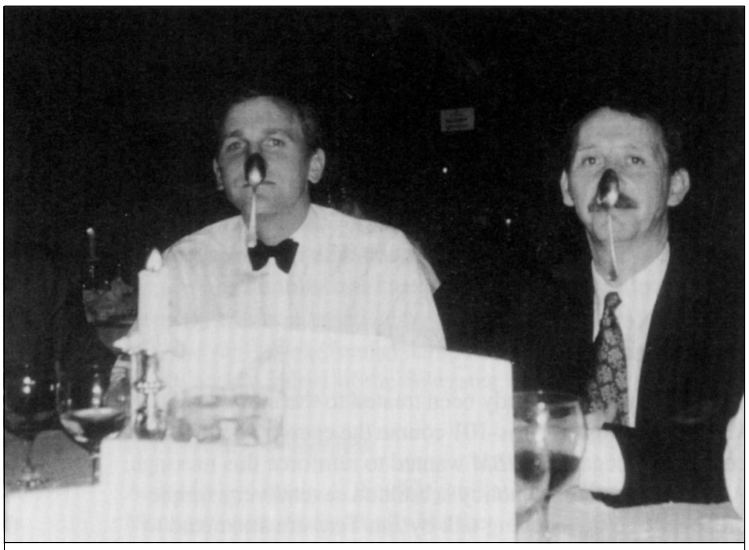
The approach adopted by *PC Magazine* was somewhat less scientific. The *PC Magazine* reviews weighted the usability of the software much more highly, explained Rupert Goodwins. Goodwins' virus detection tests were undoubtedly less rigorous, but gave his readers an idea of the 'feel' of the product. Goodwins then faced a barrage of questions from the more technically oriented members of the audience.

The ideal way to review anti-virus software has yet to be discovered, but such open discussions lead the way to better reviews for us all - the final recipe for the perfect review probably being a mixture of the *VTC's* scientific zeal and *PC Magazine's* 'touch and feel'.

New Virus Trends

Noticeably absent from this year's conference were some of the heavyweight technical papers presented in Edinburgh: hopefully there will be a stronger technical flavour to next year's event. However, the technical presentations were still one of the conference highlights.

One depressingly accurate talk was supplied by Tim Twaits, of *Sophos*. This examined a range of virus construction toolkits which seem to have grown in number overnight. Twaits cautioned that although the toolkits did not present too large a threat at this time, more 'products' were doubtless in the pipeline.



Schwartau recommends using a combination of security measures...
...delegates test his theory after the Gala Dinner.

One increasingly popular technique used for combating viruses is heuristic analysis - a method which has long been surrounded by an aura of black magic. Fortunately, Frans Veldman from *ESaSS* was intent on demystifying the entire heuristic procedure and explained to delegates how his company approached the issue... and unbelievers will be pleased to learn that there were no rams' heads, black candles or Latin incantations involved!

Blue Notes and Red Lights

On a closing note, the conference was not all work. With the venue being so close to the very heart of Amsterdam, there was much sightseeing and merry-making after hours.

The gala dinner proved to be less inflammable but at least as enjoyable as last year. Held in the Winter Garden restaurant at the hotel, the evening comprised a combination of fine food, music and entertainment, by the very capable magicians John and Saxon. The high point of the event was watching Vesselin Bontchev being placed on a working guillotine, although this was rivalled by the sight of *CPAV* product manager Tori Case seemingly floating in the air. The magician was not open to any bribes regarding either of his helpers' personal safety, and both Tori and Vesselin survived the evening unscathed!

After these excitements, the band led the party on until 1.00am - joined for the last few numbers by master saxman Jim Bates and the Editor of *VB*. 'It would never have happened in my day!' *Virus Bulletin's* erstwhile Editor, Edward Wilding, muttered darkly.

Once again, thanks are due to Petra Duffield, who consistently produces perfectly organised conferences, and all her helpers. Several people deserve the *Virus Bulletin* award for dedication well beyond the call of duty: namely Karen Richardson, Victoria Lammer, Rosalyn Rega at *Expotel International Groups* and all the staff at *Crypsys*.

Thanks are also well earned by the speakers, but particularly by all the delegates, whose lively discussions make the *Virus Bulletin* conference the event it is. Where will the conference be next year? Well - watch this space, as great plans are afoot...